

民生用LSIへの搭載を想定した低コストの1回書き込み型メモリ・コアを開発

オンチップOTPROM，セキュリティ，アナログ・トリミングなどに利用可能

Charles Ng

筆者ら（米国Kilopass Technology社）は，1回書き込み型の不揮発メモリ・コアを開発した．CMOS技術で製造できるため，最先端プロセスのLSIに容易に搭載できる．また，フラッシュ・メモリなど，ほかの不揮発メモリと比べて製造コストが安い．例えば，コストに厳しい民生用LSIにおけるファームウェアや暗号かぎの格納，アナログ・トリミング，液晶ドライバの特性調整などの用途を想定して開発した．（編集部）

システムLSI（SOC：system on a chip）の特徴として，「プロセス・ノードの縮小が進む」，「集積度が向上する」，「再利用を促進するため，シリコンIP（intellectual property）の搭載が重視される」といったことが挙げられます．さらに，もう一つの傾向として，「LSI上のメモリの比率が増加する」こともあります．多くの場合，ディジタルおよびミックスト・シグナルのシステムLSIにはさまざまな情報を格納したメモリ・コアが組み込まれています．

● 民生用では安価な不揮発メモリ・コアが求められる

システムLSIに組み込まれるメモリ・コアの一部は不揮発性です．つまり，メモリ・コアに格納された情報はチップの電源がOFFになってもそのまま保持されます．SRAMコアや，その後現れたサイズの小さいDRAMコアの技術は，不揮発メモリ・コアと比べて歴史は長いものの，電源がOFFになると格納された情報が失われるという問題があります．このため，チップの電源がOFFになっても情報が保持され続けなければならないプログラムやデータ，ユーザ情報の格納という目的にSRAMコアやDRAMコアを利用することはできません．

単体のメモリLSIとしてEPROM（erasable and programmable read only memory）が1980年代後半に登場しました．これは消去可能，かつプログラム可能であることから，情報を何度でも書き換えることができました．このデバイスは，チップ・パッケージ上の石英ガラスの消去窓からUV（紫外線）光を照射することで情報を消去します．例えばプロセッサ・コアで使用されるブート・コードやプログラムを格納するという目的に最適でした．OTPROM（one time programmable read only memory）と呼ばれる窓のない安価なメモリLSIも登場しました．これはEPROMと異なり，1回だけプログラムできるメモリLSIです．

マイクロプロセッサLSIにOTPROMコアを組み込むことも可能です．ただし，特別なフォトマスクや製造工程が必要となります．製造コストが割高になるため，OTPROMを内蔵することは少ないようです．

1990年ごろ，フラッシュ・メモリが登場しました．フローティング・ゲート技術を用いたフラッシュ・メモリ・セルの値は再設定可能です．例えば，そのデバイスがシステムに実装されている状態で，何度でも繰り返し書き換えることができます．1990年代の初期には，EPROMよりもNOR型フラッシュ・メモリが大量に出荷されるようになりました．フラッシュ・メモリはシステムLSIにも組み込まれましたが，この場合は製造コストが増大します．現在，プロセッサなどの外付けメモリには，かつてのEPROMやEEPROMに代わってフラッシュ・メモリがよく使われています．

従来の製造プロセスにいくつかの工程を追加しただけでは，チップ（CMOS論理LSI）上にフラッシュ・メモリやEPROM，EEPROMを組み込むことはできません．そのため，こうした不揮発メモリ・コアの供給は，最先端の標

準CMOS論理プロセスのリリースに対していつも遅れがちです．残念ながらこのような問題が存在するため，民生機器向けLSIにこうした不揮発メモリ・コアを気軽に搭載することができません．というのは，こうした用途では製品コストを引き下げるため，最先端のプロセスを利用する必要があるからです．

不揮発メモリ・コアのもう一つのタイプであるROMは安価で小型ですが，別の問題を抱えています．マスクROMは，チップの製造過程で「ハード・ワイヤード的に」プログラムする必要があるため，後で情報を書き換えたり，派生品展開に対応することができません．つまり，ROMにはフラッシュ・メモリのような柔軟性はありません．

筆者ら（米国Kilopass Technology社）は低コスト，セキュリティの確保，小型化を実現した新しいタイプのワンタイム・プログラマブル（1回書き込み型）の不揮発メモリ技術「XPM」を開発しました．以下では，このXPMについて解説します[注]．

● メモリ・セルはMOSトランジスタ

フラッシュ・メモリの場合，フローティング・ゲートに電荷を注入し，トンネル効果を利用することで‘1’と‘0’の値を格納します．一方，XPMでは，メモリ・セルにチャネル長が短いMOSトランジスタを使用しています．これは，プログラムされていない（書き込み前の）状態ではコンデンサ（開回路）として働きます．短い電圧パルスを用いてプログラムするとゲート酸化膜が破壊され，トランジスタは抵抗（閉回路）のようにふるまいます（**図1**）．また，通常動作時に余計な漏れ電流が流れることはありません．XPMメモリ・ブロックの書き込みに必要な電流は小さく，1Mビットのメモリをほんの数s（秒）でプログラムできます．

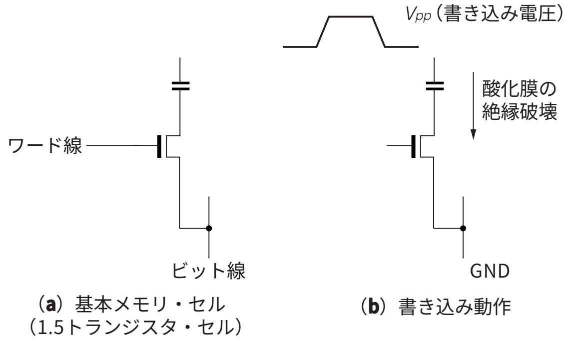


図1　XPMのメモリ・セル

プログラム電圧の短いパルスがトランジスタの酸化膜を破壊し，開回路（コンデンサ）から閉回路（抵抗）に変わる．

XPMアレイにおいて，選択された行と列のビット線とワード線に正しくバイアスをかけると，その行と列に対応したメモリ・セルがプログラムされます．同じように，プログラムされた情報を読み取る動作では，アレイ内の選択済みの行および列と，未選択の行および列に異なる電圧をかけます．これにより，アレイ上のどのセルがプログラムされているかを識別します．

XPMセルは，一見するとFPGAに使われているアンチヒューズ（通常は絶縁状態にあり，プログラム電圧を加えることにより接続状態に変わるヒューズ）のようですが，実際には従来型のアンチヒューズとは構造が異なります（稿末のコラム「FPGA/PLDとXPM技術の接点」を参照）．アンチヒューズは通常，二つの金属層間に配置された特殊な誘電体（アモルファス・シリコンの場合もある）で構成されています．プログラムすると，アンチヒューズは接続（スイッチ）を閉じます（ヒューズのように開くのではない）．

XPMもプログラムの後で接続を閉じるという点ではアンチヒューズ技術とよく似ています．しかし，現行のアンチヒューズ技術と異なり，XPMセルの接続は，金属層の間ではなくCMOSトランジスタのゲート酸化膜において行われます．XPMセルは基本的に標準のCMOSトランジスタで構成されているため，CMOS論理LSIと同じプロセス技術で製造できます．

● 従来型の不揮発メモリと比較する

XPMとそのほかの不揮発メモリ（ROM，EPROM，フラッシュ・メモリ）の比較を**表1**に示します．

1）ROMとの比較

ROMには，サイズが小さく消費電力が少ない，標準のCMOSプロセスで実装できるといった利点があります．ROMはプロセス・ノードの縮小に容易に対応できます．そのため，新しいプロセスが利用可能になると，直ちにROMを使用できます．

ROMをチップ上の不揮発メモリとして見たときの最大の問題は，マスク・プログラム方式であり，チップ製造時に構成が固定されることです．ROMコアのいずれの情報も「ロック」されているので，フォトマスクを変更してもう

注：XPMについての国内の問い合わせ先は，丸紅ソリューション（http://www.msol.co.jp/），TEL03-5778-8551．

表1
XPMとそのほかの不揮発メモリ技術

	ROM	EPROM	フラッシュ・メモリ	XPM
プロセス	標準的なCMOS論理プロセス	専用プロセス	専用プロセス	標準的なCMOS論理プロセス
プロセス世代	最先端	2～3世代遅れる	2～3世代遅れる	最先端
プロセスのスケーラビリティ	あり	なし	なし	あり
データの書き込み	マスクで書き込む	ユーザの手元で書き込む	ユーザの手元で書き込む	ユーザの手元で書き込む
ホストICの性能	高い	低い	低い	高い
読み出し速度	高速	やや高速	低速	やや高速
追加のウェハ・コスト	0	約30%	約50%	0
電力消費	低い	やや高い	やや高い	やや高い
信頼性	高い	やや高い	やや高い	高い

一度製造ラインを稼働させないかぎり，情報を変更することはできません．

今日のLSIには開発期間の短縮が要求されており，フィールド・プログラマブル（ユーザの手元でプログラム可能）でないと，こうした要求にはこたえられません．民生用LSIの機能は頻繁に更新され，ときには3カ月おきに変わることもあります．市場の要求はデバイスを製造するたびに変化するかもしれません．

ここで，プロセッサのファームウェアがROMに格納される例を考えてみましょう．システムLSIの一般的な設計フローでは，ファームウェアの開発工程がプロジェクト全体のボトルネックになっています．LSIのハードウェアの設計が終わる前に，ファームウェアの開発が完了することはありません．これは，通常，1枚または複数枚のマスクに対して，少なくとも1回の再設計が必要になるということであり，新しいマスクを使ってLSIを製造するための余分な時間も必要になるということも意味します．

ファームウェアの修正によってマスクROMの内容が変わるたびに開発費（NRE：non-recurring expenses）が必要になります．これは，今日主流のプロセスにおいては多大な負担であり，プロセス・ノードが縮小するたびに経費の金額がはね上がります．また，今日の大規模な半導体工場では，マスクを変更するたびに2～3ヵ月を超える製造期間が必要になります．加えて，マスクROMを搭載したチップの場合，チップのバージョンごとに異なるROM（例えば，各種の機能の組み合わせや異なるファームウェアを格納）が必要になり，これらの在庫を管理するため，実質的にチップのコストが増大します．

2）EPROM（紫外線消去型）との比較

これまでEPROMを使用していたアプリケーションの多くは，フラッシュ・メモリに移行しつつあります．これは当然のことで，フラッシュ・メモリはEPROMに勝る製造プロセス上の利点を備えており，また，アクセス速度も高速です．

3）フラッシュ・メモリとの比較

フラッシュ・メモリ技術はすでに成熟期を迎えており，多くのアプリケーションや製品で実証済みの技術と言えます．ただし，民生用LSIに組み込むフラッシュ・メモリ・コアには三つの問題点があります．すなわち，「コストが高い」，「最新のプロセス・ノードに対応することが困難」，そして「サイズが大きい」という問題です．

PDAやMP3プレーヤ，ディジタル・カメラ，ビデオ・カメラ，ゲーム機，携帯電話などの製品の利幅はきわめて小さくなっています．コストに厳しいこれらの製品をターゲットとしたLSIと，そうでないLSIのコストの差はほんの数セントしかありません．CMOS論理LSIにフラッシュ・メモリ・コアを組み込もうとすると，余分なマスクと製造工程が必要になり，LSIの製造コストは約50%も高くなります．

加えて，フラッシュ・メモリには最新のプロセス・ノードに追随する（遅れずについていく）ことが難しいという欠点があります．より微細なプロセス・ノードに移行する利点は，より多くの機能を同一サイズのチップに組み込めること，または，現在の機能をよりサイズの小さいチップで実現することにより，コストを低減できることにあります．いずれのケースも，民生機器メーカにとっては非常に魅力的な利点です．

フラッシュ・メモリやそのほかの電荷蓄積型のフローティング・ゲート技術には，電荷を蓄積するがゆえの制限があります．トランジスタの酸化膜が薄くなるにつれて，トンネル効果によって電荷が消失してしまうのです．このため，フラッシュ・メモリの電荷蓄積技術では，ウェハのトンネル酸化膜の厚みについて80～85Å（オングストローム）という寸法制限が設けられています．この値は，いったん電荷が蓄積され，フラッシュ・メモリが確実にその電荷を保持するために必要なトンネル酸化膜の厚みです．現在のCMOS論理ゲートの酸化膜はこれよりはるかに薄く，30Å程度です．さらに，先端のプロセス・ノードで製造されたチップではトンネル効果が起こる電圧が低くなるため，記憶セルの素子（トランジスタ）間の距離に制限が生じます．つまり，フラッシュ・メモリでは，トランジスタ間にある一定の距離を置く必要があります．このため，フラッシュ・メモリは，最先端のプロセスで製造することが困難なのです．

● 1回書き込み型でもフィールド・アップグレードは可能

フラッシュ・メモリやEPROMなど，書き換え可能な不揮発メモリを使用すると，製品が市場に出てからでもシステムを修正したり，ソフトウェアのアップグレードやそのほかの修正に対応できます．一方，従来型の書き換え可能な不揮発メモリをXPMのような1回書き込み型で代替できる局面もいろいろとあります．

図2は，XPMを使ってファームウェアのフィールド・アップグレードを行う方法を示しています．XPMメモリ・コアには，ファームウェア・コードを格納した（プログラム済み）セクタのほかに，未使用のセクタがあります．ファームウェア・モジュールの一つ（モジュールB）をアップグレードするため，未使用のセクタを新たにプログラムします．そして，アップグレードしたモジュール（モジュールB*）と，制御論理によって切り替えるようにしています．

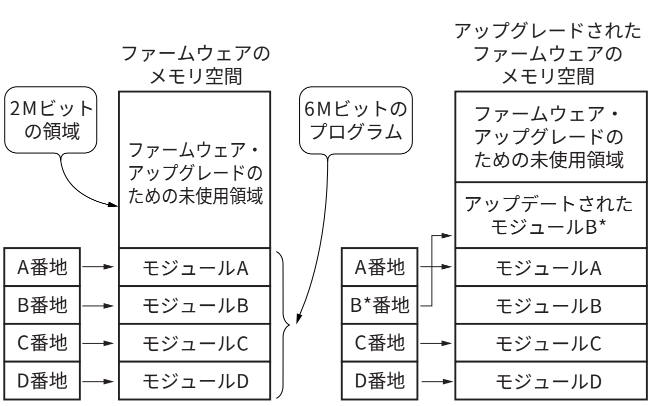


図2　ファームウェアをアップグレードする方法
XPMメモリにプログラムしていないセクタを残しておけば，そのセクタに新しいアップグレード・データを書き込むことによって，ファームウェアを更新できる．

● 不正アクセスに強いメモリ技術

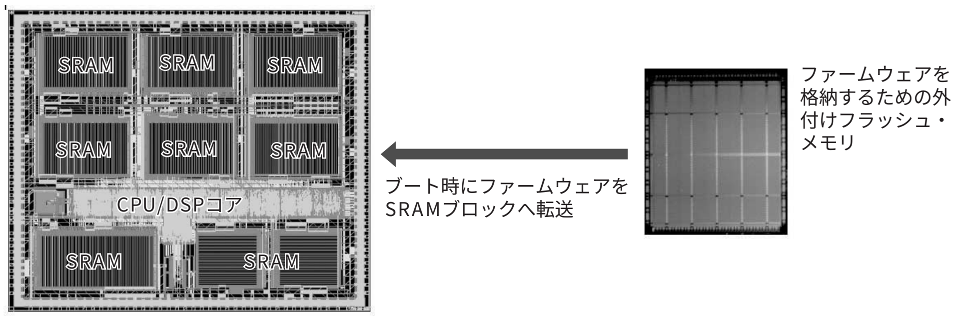
不揮発メモリ・コアにセキュリティ情報を格納することは，現在，民生用機器の開発者にとってきわめて重要な問題となっています．LSIに格納されたファームウェアやアプリケーション・ソフトウェアは，開発元の貴重な知的財産であり，不正なアクセスから保護する必要があります．同じように，ユーザの個人情報やそのほかの機密データも第三者による読み取りや改変から保護する必要があります．

外付けした不揮発メモリのビット・ストリームは不法に読み取られる可能性があります．SRAMデバイスの情報を暗号化した場合でも，チップ上または外付けのEPROMやフラッシュ・メモリから暗号かぎを「盗まれる」可能性があります．電圧コントラスト・スキャンと呼ばれる方法を利用すると，これらのメモリのセルに格納された電荷を比較的簡単に読み取れるからです．

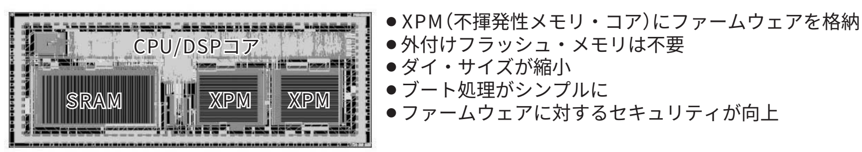
XPM技術は，‘1’と‘0’を区別するために蓄積電荷を利用しておらず，電気的，電磁誘導的，あるいは磁気的な方法によってデータを読み取ることができません．さらに，XPMセルがプログラムされているかどうかを視覚的に検出することもできません．また，アンチヒューズ方式のFPGA技術などと異なり，セルのリバース・エンジニアリングを行うこともできません．このため，XPMメモリ・コアは，いずれの不揮発メモリ技術と比べても，より高度なセキュリティを確保できます．ファームウェアやID，バイオメトリック，および個人情報などの格納に向いた技術であると言えます．

● 暗号かぎの格納やアナログ特性の調整などに使える

システムLSI上にXPMメモリ・コアを集積することにより，チップ上のROMやEPROM，フラッシュ・メモリなどが抱える問題が解消されます．**図3**は，プロセッサLSIにXPMメモリ・コアを導入することで，2チップ構成から1チップ構成に変わった例のイメージを示しています．システムLSIのサイズは小さくなり，必要なSRAMの容量が減り，さらにシステム・コストが低減します．そして同じ



（**a**）2チップ構成



（**b**）XPMを利用（1チップ構成）

図3　ファームウェアの格納にXPM技術を利用した場合のイメージ
ファームウェアの格納にXPM技術を利用すると，プロセッサ・コアを搭載するシステムLSIのサイズが縮小する．また，外付けの不揮発メモリも不要になる．

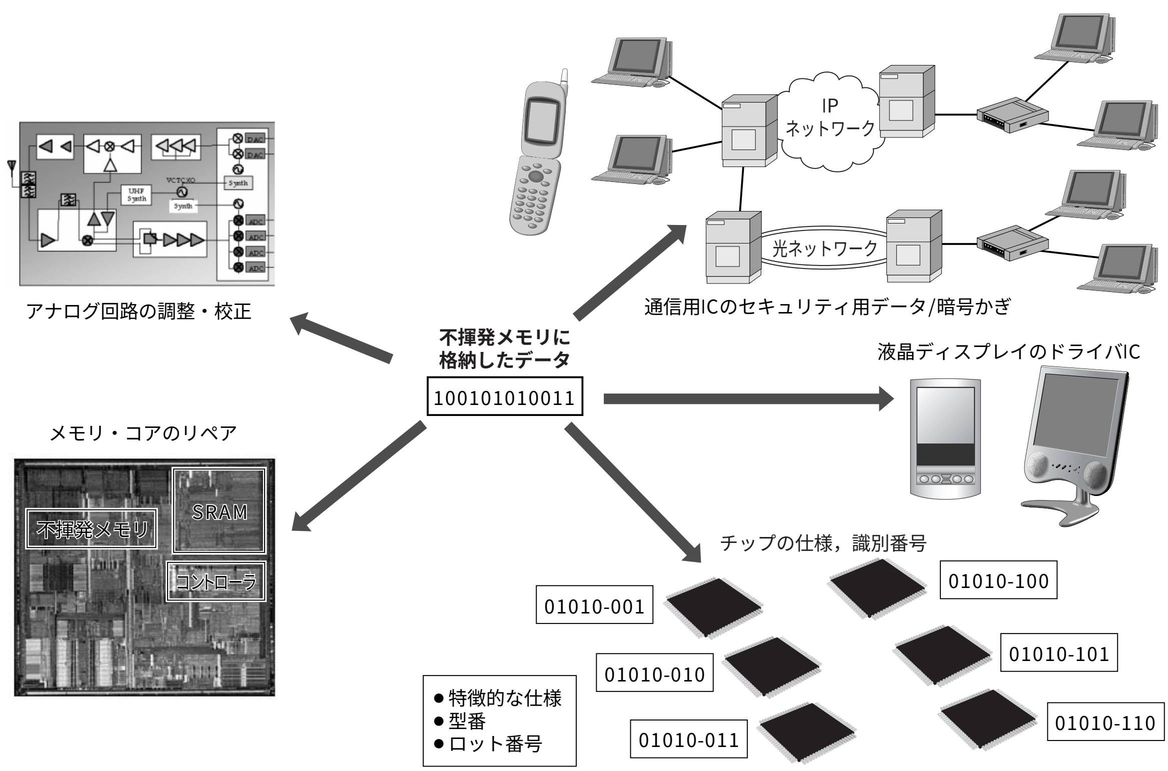


図4　小容量のXPMメモリ・コアのアプリケーション例
XPM技術は，小容量の不揮発メモリ・コアが必要ないくつかのアプリケーションにも対応できる．

くらい重要なことは，2チップ構成のときより格納されたコードに対するセキュリティが向上していることです．

図4は，容量の小さいXPMが使用されるアプリケーションの例を示しています．アプリケーションの一つはセキュリティであり，例えばXPMメモリ・コアに暗号かぎを格納することが考えられます．チップ内に暗号かぎと機密

データを格納すれば，不法にかぎを取り出すことは非常に難しくなります．

容量の小さいXPMのもう一つのアプリケーションは，少数のデータ・ビット（100ビット未満）をアナログ・アンプやそのほかの高精度アナログ・チップに組み込み，特性をディジタル的に調整できるようにする用途です．

従来のアナログ・トリミング，すなわち薄膜抵抗をレーザ・トリミングする方法や，金属やポリシリコンの接続（ヒューズ）をレーザでカットする方法，ツェナ・ダイオードの破壊を利用して抵抗を調整する方法，電流によってポリ・ヒューズを開放する方法，EPROMやEEPROMにデータ・ビットを格納し，D-Aコンバータを制御して電流や電圧を調整する方法は，それなりに効果を上げてきました．ただし，これらの手法にはそれぞれ個別の欠点があります．例えば，チップのコストや信頼性，調整の精度などに悪影響を及ぼす可能性があります．

XPMを使用してアナログ回路のトリミングを行えば，幅広いプロセス・ノードに柔軟に対応できます．また，非常に小さい領域にデータ・ビットを格納できるので，製造コストはほとんど上昇しません．

このほか，数ビット分のデータを格納するXPMメモリ・コアをLCD（液晶ディスプレイ）ドライバに搭載すれば，各ドライバをそれぞれが制御するLCDやプラズマ・ディスプレイの特性に合わせて調整できます．これらのいずれのアプリケーションにおいても，製造工場のそれぞれの作業フローに合わせて，自動あるいは手動で不揮発メモリをプログラムすることができます．

XPMメモリ・コアは，製品が市場に出てから（ユーザの手元で）プログラムすることが可能です．そのため，遠隔地からデータを書き込むような用途にも使えます．例えば，暗号かぎを更新したり，アクセス・コードを変更したり，あるいは携帯電話のPIN（personal identification number；商品やサービスの購入に使用する番号）を修正することも可能です．LCDドライバにXPMメモリ・コアを集積すれば，組み立ての完了したディスプレイの校正を製造ラインの最終工程で実施することもできます．また，家庭にディスプレイを設置するときに，専門家が購入者の好みを考慮してディスプレイの特性を調整する用途にも利用できます．

Charles Ng
米国Kilopass Technology社

<筆者プロフィール>
Charles Ng．Kilopass社 Vice-President of Worldwide Sales & Marketing．Kilopass社の前は，米国Cadence Design Systems社や米国VLSI Technology社において管理職を務める．米国California Institute of Technologyでコンピュータ工学の学士号と修士号を取得．また，University of California at BerkeleyでMBA（経営学修士）を取得．

■COLUMN FPGA/PLDとXPM技術の接点

Kilopass社の創設者で，会長を務めるJack Peng氏は，大学在学中，半導体メモリについて研究していました．米国University of Marylandにおける同氏の博士論文は，メモリ・デバイスの物理学を取り扱ったものでした．大学卒業後，同氏は20年以上，半導体の研究開発に携わりました．Kilopass社を創設する前は，米国Actel社，米国GateField社，および米国AMD（Advanced Micro Devices）社でEPROM，フラッシュ・メモリ，EEPROM，PLD，そしてフラッシュ・ベースFPGAの開発を担当していました．

GateField社に在籍していたころ，Peng氏はフラッシュ・ベースFPGAの開発に取り組んでいました．同氏は過去にレーザ光で読み取るIDカードの開発に取り組んだことがありましたが，アプリケーションの実現にコストがかかりすぎると考えていました．そして同氏は，今後，高密度でセキュリティを確保できる低コストのメモリ技術が必要になると考えました．ただし，低コストの民生機器ではフラッシュ・メモリはコストがかかりすぎること，また民生用LSIを製造するプロセス技術に一般的なアンチヒューズ技術を簡単には流用できないことも認識していました．

同氏は，ある既存のメモリ技術に対して酸化膜のテストを実施していたとき，適切な電圧ストレスの条件下でトランジスタのゲート酸化膜の破壊を再現でき，かつこれを製造できる方法を思いつきました．これが，XPM技術の原点となりました．

2001年初めに，Peng氏は，自分の研究の成果を持ってKilopass社を創設しました．この会社はその年の年末には活動を開始しました．